FIG. 1

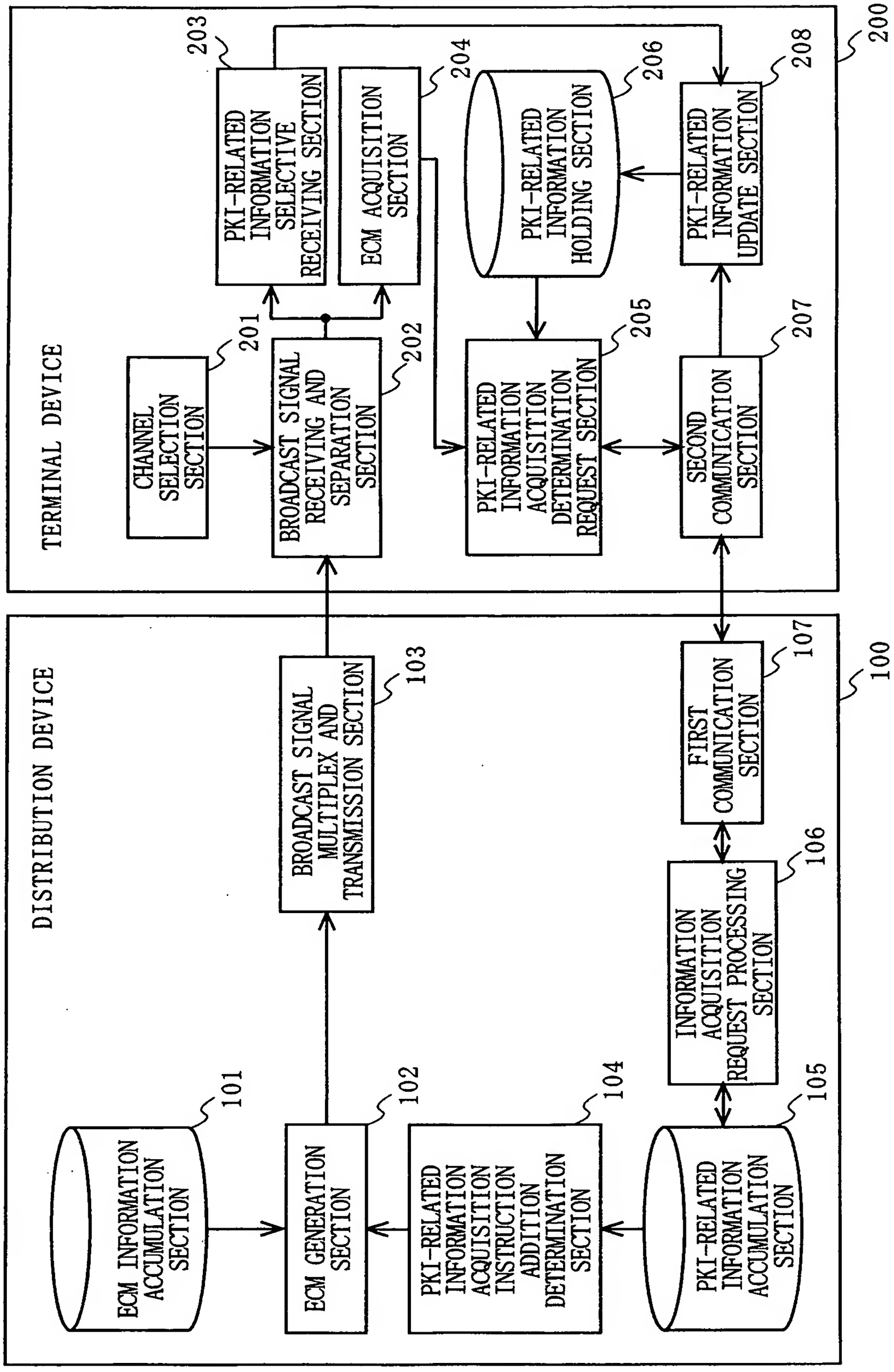
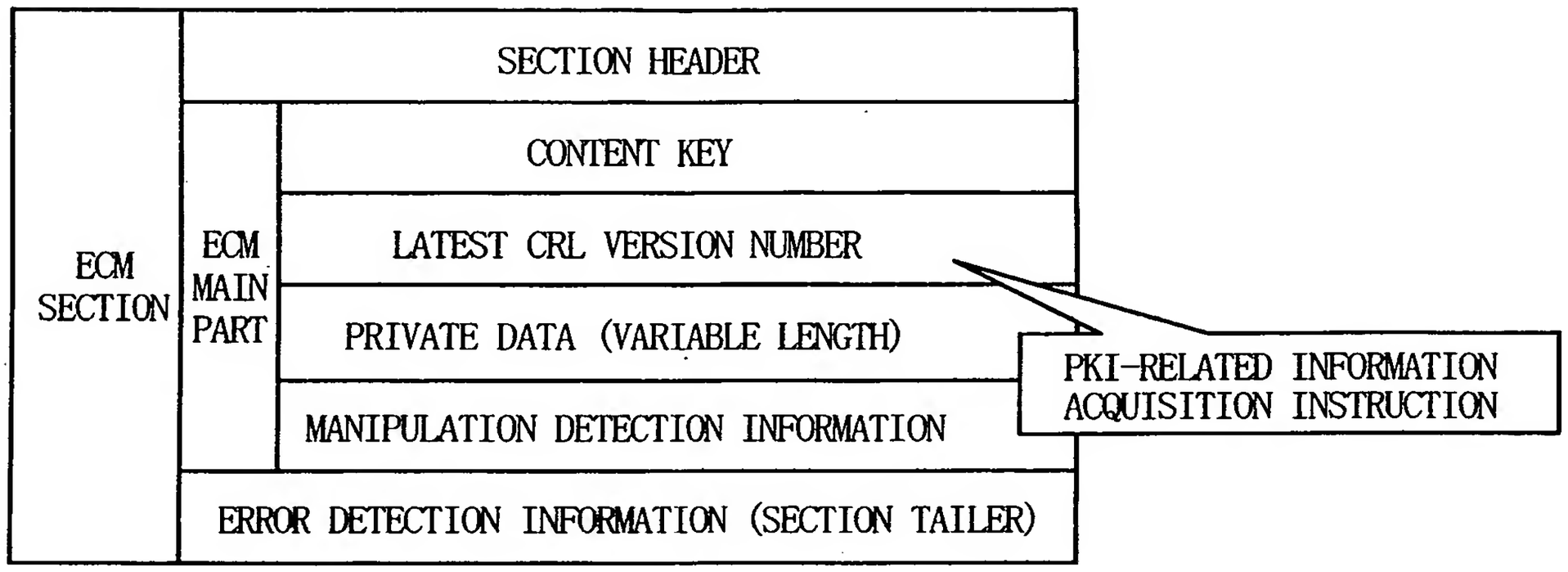

DISTRIBUTION DEVICE
TERMINAL DEVICE
100
200
ECM INFORMATION ACCUMULATION SECTION
101
ECM GENERATION SECTION
102
BROADCAST SIGNAL MULTIPLEX AND TRANSMISSION SECTION
103
PKI-RELATED INFORMATION ACQUISITION INSTRUCTION ADDITION DETERMINATION SECTION
104
PKI-RELATED INFORMATION ACCUMULATION SECTION
105
INFORMATION ACQUISITION REQUEST PROCESSING SECTION
106
FIRST COMMUNICATION SECTION
107
CHANNEL SELECTION SECTION
201
BROADCAST SIGNAL RECEIVING AND SEPARATION SECTION
202
PKI-RELATED INFORMATION ACQUISITION DETERMINATION REQUEST SECTION
205
SECOND COMMUNICATION SECTION
207
PKI-RELATED INFORMATION SELECTIVE RECEIVING SECTION
203
ECM ACQUISITION SECTION
204
PKI-RELATED INFORMATION HOLDING SECTION
206
PKI-RELATED INFORMATION UPDATE SECTION
208

FIG. 2


ECM SECTION
SECTION HEADER
ECM MAIN PART
CONTENT KEY
LATEST CRL VERSION NUMBER
PRIVATE DATA (VARIABLE LENGTH)
MANIPULATION DETECTION INFORMATION
ERROR DETECTION INFORMATION (SECTION TAILER)
PKI-RELATED INFORMATION ACQUISITION INSTRUCTION

F I G. 3

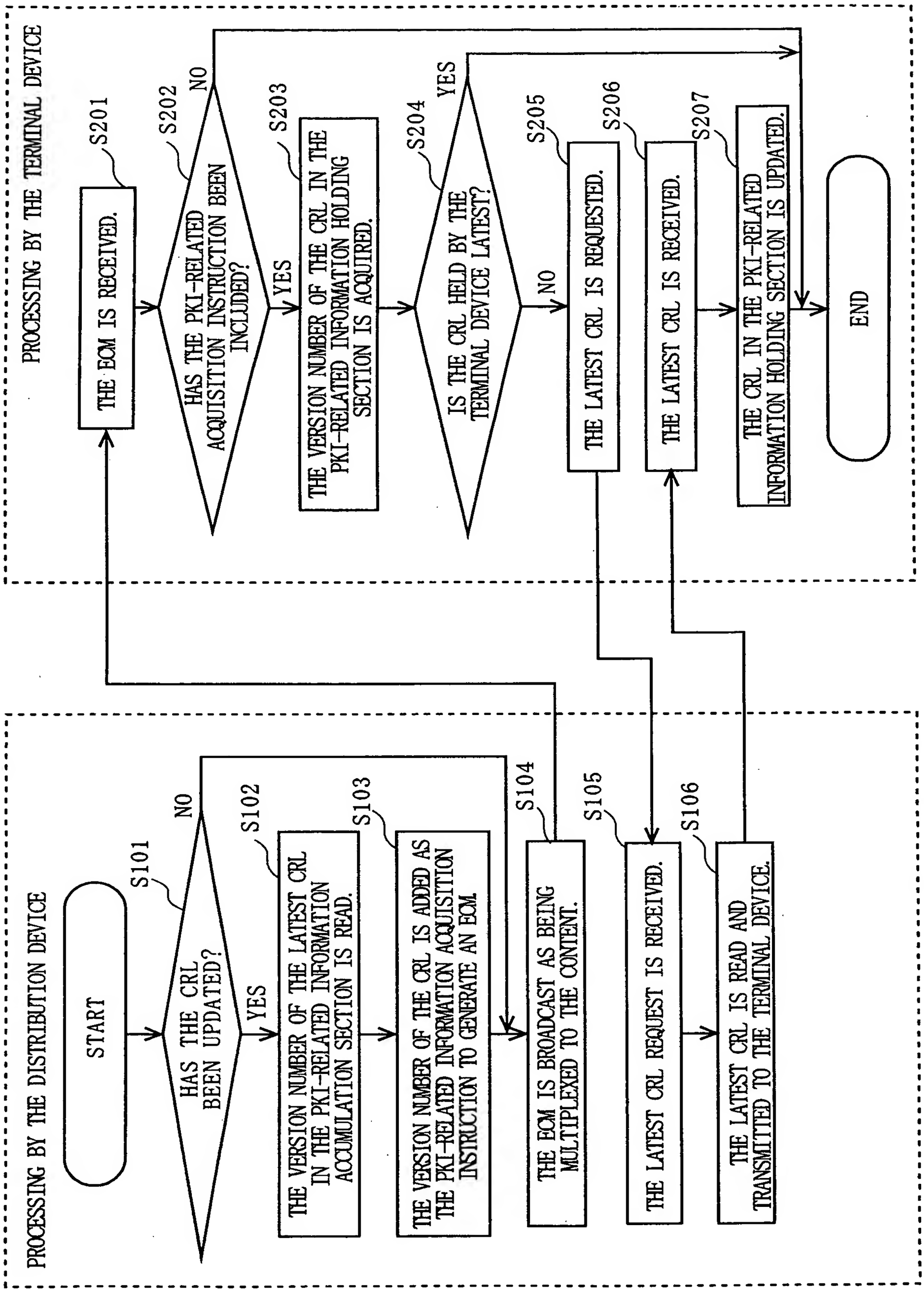

PROCESSING BY THE TERMINAL DEVICE
S201
THE ECM IS RECEIVED.
S202
HAS THE PKI-RELATED ACQUISITION INSTRUCTION BEEN INCLUDED?
NO
YES
S203
THE VERSION NUMBER OF THE CRL IN THE PKI-RELATED INFORMATION HOLDING SECTION IS ACQUIRED.
S204
IS THE CRL HELD BY THE TERMINAL DEVICE LATEST?
YES
NO
S205
THE LATEST CRL IS REQUESTED.
S206
THE LATEST CRL IS RECEIVED.
S207
THE CRL IN THE PKI-RELATED INFORMATION HOLDING SECTION IS UPDATED.
END
PROCESSING BY THE DISTRIBUTION DEVICE
START
S101
HAS THE CRL BEEN UPDATED?
NO
YES
S102
THE VERSION NUMBER OF THE LATEST CRL IN THE PKI-RELATED INFORMATION ACCUMULATION SECTION IS READ.
S103
THE VERSION NUMBER OF THE CRL IS ADDED AS THE PKI-RELATED INFORMATION ACQUISITION INSTRUCTION TO GENERATE AN ECM.
S104
THE ECM IS BROADCAST AS BEING MULTIPLEXED TO THE CONTENT.
S105
THE LATEST CRL REQUEST IS RECEIVED.
S106
THE LATEST CRL IS READ AND TRANSMITTED TO THE TERMINAL DEVICE.

FIG. 4

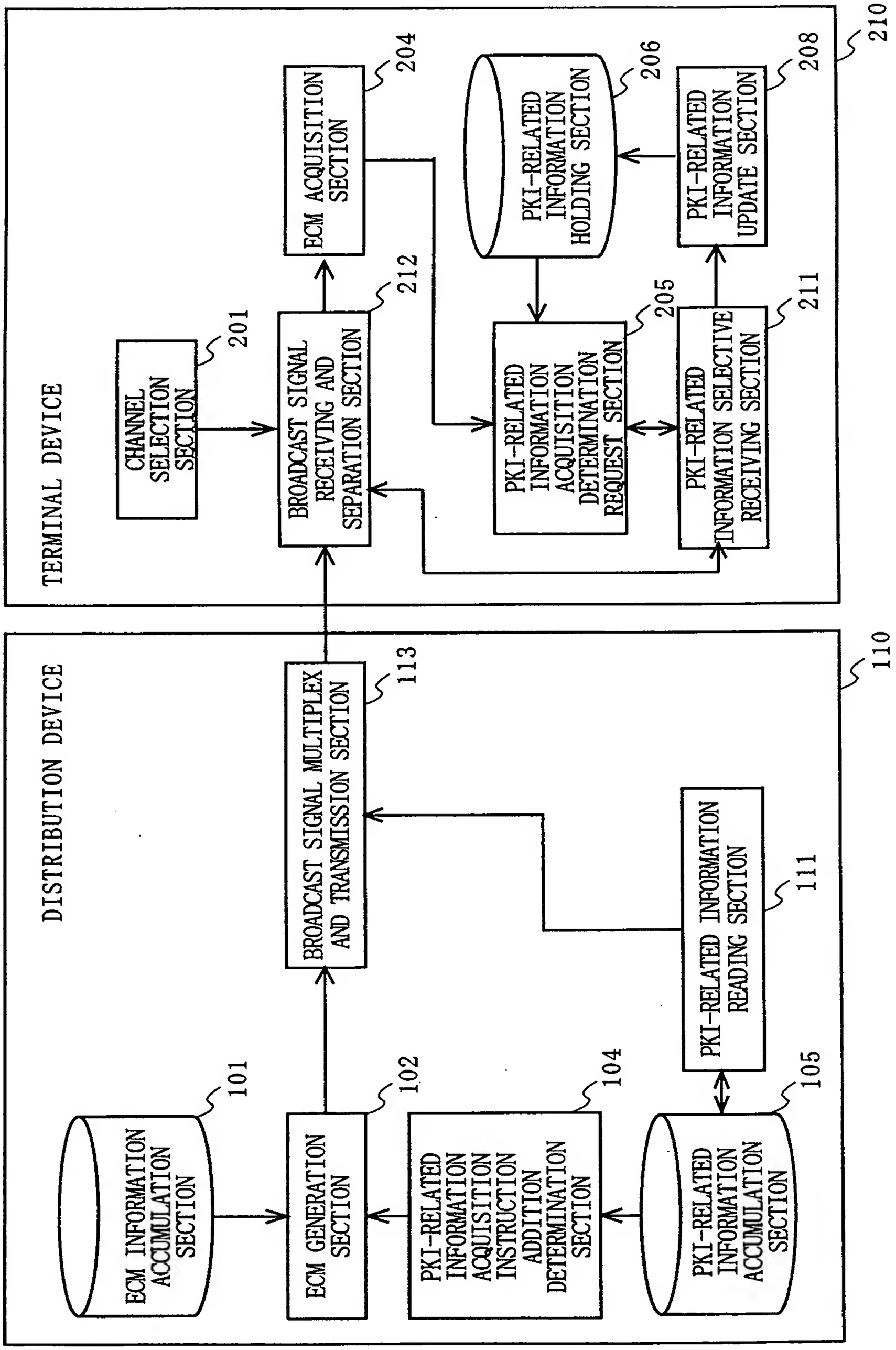

DISTRIBUTION DEVICE
110
BROADCAST SIGNAL MULTIPLEX AND TRANSMISSION SECTION
113
PKI-RELATED INFORMATION READING SECTION
111
ECM INFORMATION ACCUMULATION SECTION
101
ECM GENERATION SECTION
102
PKI-RELATED INFORMATION ACQUISITION INSTRUCTION ADDITION DETERMINATION SECTION
104
PKI-RELATED INFORMATION ACCUMULATION SECTION
105
TERMINAL DEVICE
210
ECM ACQUISITION SECTION
204
PKI-RELATED INFORMATION HOLDING SECTION
206
PKI-RELATED INFORMATION UPDATE SECTION
208
CHANNEL SELECTION SECTION
201
BROADCAST SIGNAL RECEIVING AND SEPARATION SECTION
212
PKI-RELATED INFORMATION ACQUISITION DETERMINATION REQUEST SECTION
205
PKI-RELATED INFORMATION SELECTIVE RECEIVING SECTION
211

FIG. 5

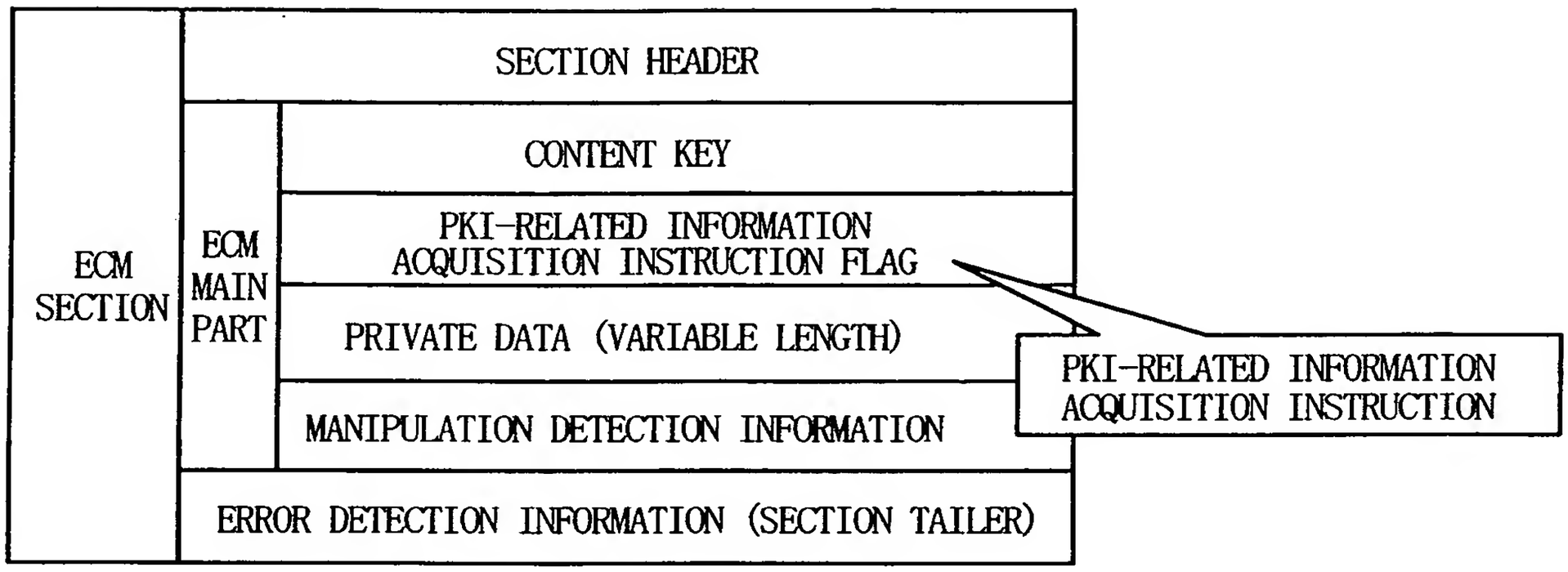

ECM SECTION
SECTION HEADER
ECM MAIN PART
CONTENT KEY
PKI-RELATED INFORMATION ACQUISITION INSTRUCTION FLAG
PRIVATE DATA (VARIABLE LENGTH)
MANIPULATION DETECTION INFORMATION
ERROR DETECTION INFORMATION (SECTION TAILER)
PKI-RELATED INFORMATION ACQUISITION INSTRUCTION

FIG. 6

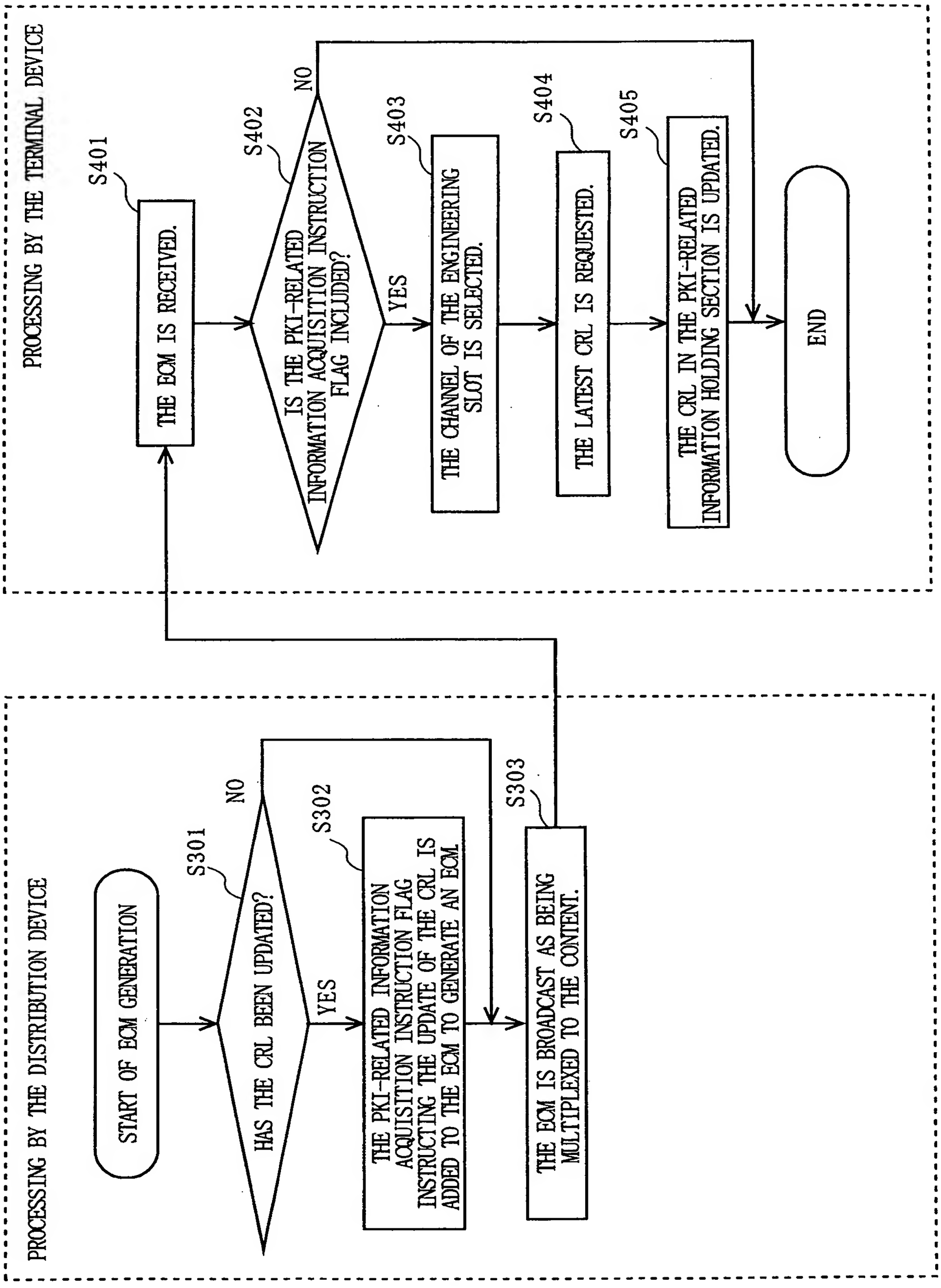

PROCESSING BY THE DISTRIBUTION DEVICE
START OF ECM GENERATION
S301
HAS THE CRL BEEN UPDATED?
NO
YES
S302
THE PKI-RELATED INFORMATION ACQUISITION INSTRUCTION FLAG INSTRUCTING THE UPDATE OF THE CRL IS ADDED TO THE ECM TO GENERATE AN ECM
S303
THE ECM IS BROADCAST AS BEING MULTIPLEXED TO THE CONTENT.
PROCESSING BY THE TERMINAL DEVICE
S401
THE ECM IS RECEIVED.
S402
IS THE PKI-RELATED INFORMATION ACQUISITION INSTRUCTION FLAG INCLUDED?
NO
YES
S403
THE CHANNEL OF THE ENGINEERING SLOT IS SELECTED.
S404
THE LATEST CRL IS REQUESTED.
S405
THE CRL IN THE PKI-RELATED INFORMATION HOLDING SECTION IS UPDATED.
END

FIG. 7

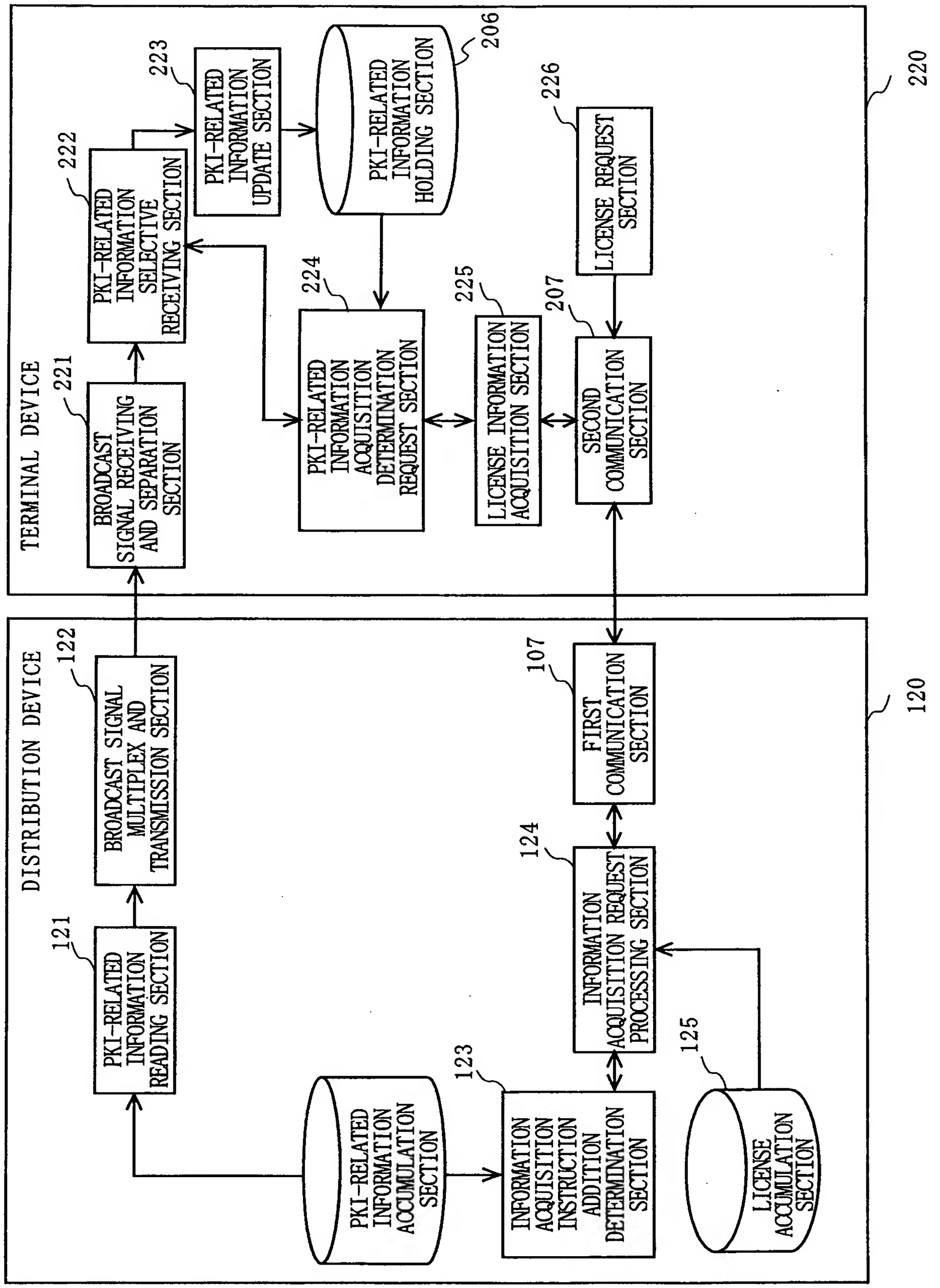

DISTRIBUTION DEVICE
122
BROADCAST SIGNAL MULTIPLEX AND TRANSMISSION SECTION
121
PKI-RELATED INFORMATION READING SECTION
PKI-RELATED INFORMATION ACCUMULATION SECTION
123
INFORMATION ACQUISITION INSTRUCTION ADDITION DETERMINATION SECTION
125
LICENSE ACCUMULATION SECTION
120
107
FIRST COMMUNICATION SECTION
124
INFORMATION ACQUISITION REQUEST PROCESSING SECTION
TERMINAL DEVICE
221
BROADCAST SIGNAL RECEIVING AND SEPARATION SECTION
222
PKI-RELATED INFORMATION SELECTIVE RECEIVING SECTION
223
PKI-RELATED INFORMATION UPDATE SECTION
206
PKI-RELATED INFORMATION HOLDING SECTION
224
PKI-RELATED INFORMATION ACQUISITION DETERMINATION REQUEST SECTION
225
LICENSE INFORMATION ACQUISITION SECTION
207
SECOND COMMUNICATION SECTION
226
LICENSE REQUEST SECTION
220

FIG. 8

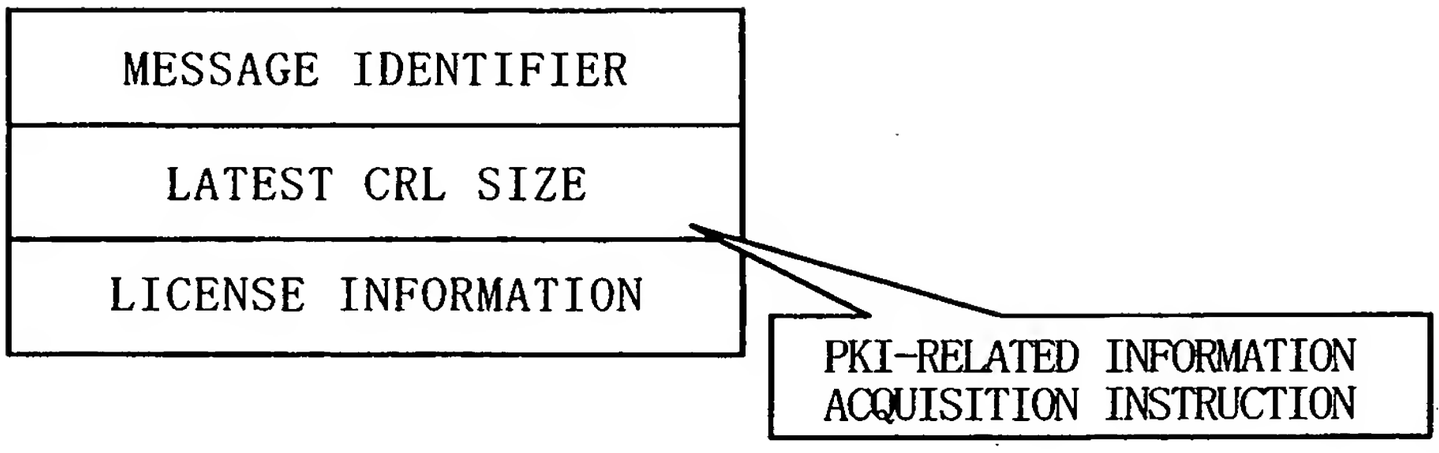
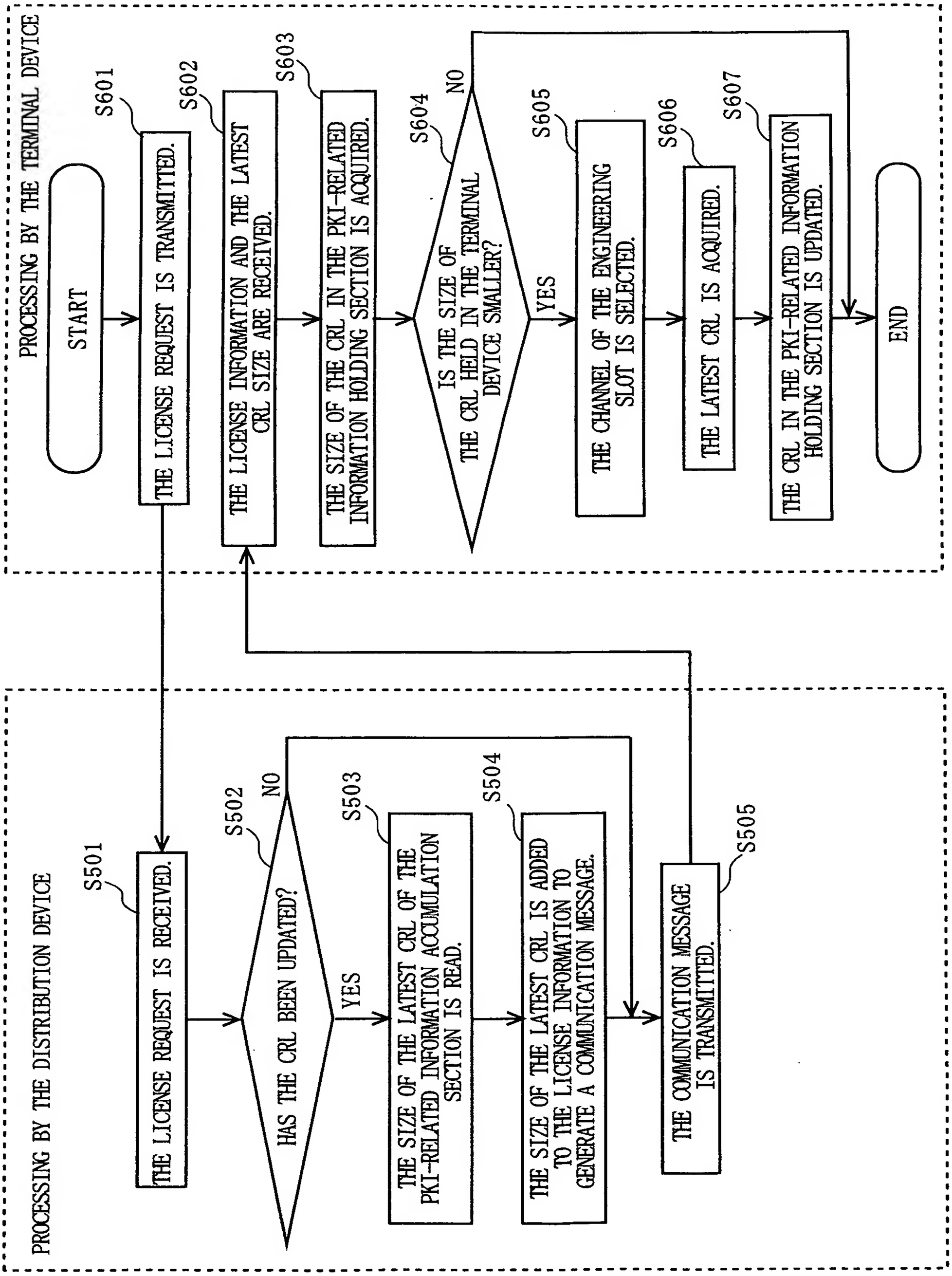

MESSAGE IDENTIFIER
LATEST CRL SIZE
LICENSE INFORMATION
PKI-RELATED INFORMATION ACQUISITION INSTRUCTION

FIG. 9


PROCESSING BY THE TERMINAL DEVICE
START
S601
THE LICENSE REQUEST IS TRANSMITTED.
S602
THE LICENSE INFORMATION AND THE LATEST CRL SIZE ARE RECEIVED.
S603
THE SIZE OF THE CRL IN THE PKI-RELATED INFORMATION HOLDING SECTION IS ACQUIRED.
S604
IS THE SIZE OF THE CRL HELD IN THE TERMINAL DEVICE SMALLER?
NO
YES
S605
THE CHANNEL OF THE ENGINEERING SLOT IS SELECTED.
S606
THE LATEST CRL IS ACQUIRED.
S607
THE CRL IN THE PKI-RELATED INFORMATION HOLDING SECTION IS UPDATED.
END
PROCESSING BY THE DISTRIBUTION DEVICE
S501
THE LICENSE REQUEST IS RECEIVED.
S502
HAS THE CRL BEEN UPDATED?
NO
YES
S503
THE SIZE OF THE LATEST CRL OF THE PKI-RELATED INFORMATION ACCUMULATION SECTION IS READ.
S504
THE SIZE OF THE LATEST CRL IS ADDED TO THE LICENSE INFORMATION TO GENERATE A COMMUNICATION MESSAGE.
S505
THE COMMUNICATION MESSAGE IS TRANSMITTED.